IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method for identifying network traffic comprising:

receiving pattern matching data;

comparing the pattern matching data with each of a plurality of patterns;

for each pattern, determining whether the pattern matching data matches the pattern;

for each pattern that the pattern matching data is determined to match, including a pattern match score corresponding to the pattern in an application protocol score associated with an application protocol with which the pattern is associated, wherein the application protocol comprises one of a plurality of application protocols and each pattern is associated with a corresponding one of the plurality of application protocols; and

concluding that a network traffic with which the pattern matching data is associated is associated with a determined application protocol that has a highest application protocol score among the plurality of application protocols.

2. (Original) A method for identifying network traffic as recited in Claim 1, wherein the pattern matching data includes application data.

3. (Original) A method for identifying network traffic as recited in Claim 1, in the event that the pattern matching data matches the pattern, further including determining a property associated with the network traffic.

4. (Canceled)

5. (Original) A method for identifying network traffic as recited in Claim 1, in the event that the data matches the pattern, further including determining a property associated with the data and assigning a score for the property.

6. (Original) A method for identifying network traffic as recited in Claim 1, in the event that the data matches the pattern, further including determining a property associated with the data; and applying a policy based on the property.

7. (Canceled)

8. (Canceled)

9. (Canceled)

10. (Original) A method for identifying network traffic as recited in Claim 1, wherein the pattern matching data includes a string selected from a packet.

11. (Original) A method for identifying network traffic as recited in Claim 1, wherein pattern matching data includes concatenated application data of a plurality of packets.

12. (Original) A method for identifying network traffic as recited in Claim 1, wherein the pattern includes a regular expression.

13. (Original) A method for identifying network traffic as recited in Claim 1, wherein the pattern includes application protocol information.

14. (Original) A method for identifying network traffic as recited in Claim 1, wherein the pattern includes commonly used port information.

15. (Original) A method for identifying network traffic as recited in Claim 1, in the event the data does not match the pattern, further comprising returning a failure indicator.

16. (Currently Amended) A method for identifying network traffic as recited in Claim 1, wherein determining whether the pattern matching data matches the pattern occurs at the beginning of a session.

17. (Original) A method for identifying network traffic as recited in Claim 1, wherein comparing the pattern matching data with a pattern is performed for each received data.

18. (Canceled)

19. (Canceled)

20. (Previously Presented) A system for identifying network traffic comprising:

an interface configured to receive pattern matching data;

a processor configured to:

compare the pattern matching data with each of a plurality of patterns;

for each pattern, determine whether the pattern matching data matches the pattern;

for each pattern that the pattern matching data is determined to match, include a pattern match score corresponding to the pattern in an application protocol score associated with an application protocol with which the pattern is associated, wherein the application protocol comprises one of a plurality of application protocols and each pattern is associated with a corresponding one of the plurality of application protocols; and

conclude that a network traffic with which the pattern matching data is associated is associated with a determined application protocol that has a highest application protocol score among the plurality of application protocols.

21. (Currently Amended) A computer program product for identifying network traffic, the computer program product being embodied in a tangible computer readable storage medium and comprising computer instructions for:

receiving pattern matching data;

comparing the pattern matching data with each of a plurality of patterns;

for each pattern, determining whether the pattern matching data matches the pattern;

for each pattern that the pattern matching data is determined to match, including a pattern match score corresponding to the pattern in an application protocol score associated with an application protocol with which the pattern is associated, wherein the application protocol comprises one of a plurality of application protocols and each pattern is associated with a corresponding one of the plurality of application protocols; and

concluding that a network traffic with which the pattern matching data is associated is associated with a determined application protocol that has a highest application protocol score among the plurality of application protocols.

22. (Canceled)

23. (New) A system for identifying network traffic as recited in Claim 20, wherein the pattern matching data includes application data.

24 (New) A system for identifying network traffic as recited in Claim 20, wherein the processor is further configured to determine a property associated with the network traffic in the event that the pattern matching data matches the pattern.

25. (New) A system for identifying network traffic as recited in Claim 20, wherein the processor is further configured to determine a property associated with the data and assign a score for the property in the event that the data matches the pattern.

26. (New) A system for identifying network traffic as recited in Claim 20, wherein the processor is further configured to determine a property associated with the data and apply a policy based on the property in the event that the data matches the pattern.

27. (New) A system for identifying network traffic as recited in Claim 20, wherein the pattern matching data includes a string selected from a packet.

28. (New) A system for identifying network traffic as recited in Claim 20, wherein pattern matching data includes concatenated application data of a plurality of packets.

29. (New) A system for identifying network traffic as recited in Claim 20, wherein the pattern includes a regular expression.

30. (New) A system for identifying network traffic as recited in Claim 20, wherein the pattern includes application protocol information.

31. (New) A system for identifying network traffic as recited in Claim 20, wherein the pattern includes commonly used port information.

32. (New) A system for identifying network traffic as recited in Claim 20, wherein the processor is further configured to return a failure indicator in the event the data does not match the pattern.

33. (New) A system for identifying network traffic as recited in Claim 20, wherein the processor is configured to determine whether the pattern matching data matches the pattern at the beginning of a session.

34. (New) A system for identifying network traffic as recited in Claim 20, wherein the processor is configured to compare the pattern matching data with a pattern for each received data.

35. (New) A computer program product as recited in Claim 21, wherein the pattern matching data includes application data.

36. (New) A computer program product as recited in Claim 21, further comprising computer instructions for determining a property associated with the network traffic in the event that the pattern matching data matches the pattern.

37. (New) A computer program product as recited in Claim 21, further comprising computer instructions for determining a property associated with the data and assigning a score for the property in the event that the data matches the pattern.

38. (New) A computer program product as recited in Claim 21, further comprising computer instructions for determining a property associated with the data; and applying a policy based on the property in the event that the data matches the pattern.

39. (New) A computer program product as recited in Claim 21, wherein the pattern matching data includes a string selected from a packet.

40. (New) A computer program product as recited in Claim 21, wherein pattern matching data includes concatenated application data of a plurality of packets.

41. (New) A computer program product as recited in Claim 21, wherein the pattern includes a regular expression.

42. (New) A computer program product as recited in Claim 21, wherein the pattern includes application protocol information.

43. (New) A computer program product as recited in Claim 21, wherein the pattern includes commonly used port information.

44. (New) A computer program product as recited in Claim 21, further comprising computer instructions for returning a failure indicator in the event the data does not match the pattern.

45. (New) A computer program product as recited in Claim 21, wherein determining whether the pattern matching data matches the pattern occurs at the beginning of session.

46. (New) A computer program product as recited in Claim 21, wherein comparing the pattern matching data with a pattern is performed for each received data.